From: [redacted]
To: OAIC - Privacy Reform Tranche 1
Subject: Practitioner input: AI connector risk and Privacy Impact Assessment methodology — PAARA Connector-DPIA Methodology
Date: Thursday, 21 May 2026 3:13:54 PM

CAUTION: This email originated from outside of the organisation. Do not click links or open attachments unless you recognise the sender and know the content is safe.

Dear OAIC Engagement Team,

I am writing to share a practitioner methodology as input to OAIC's ongoing review of guidance on privacy and commercially available AI products, and the forthcoming guidance on automated decision-making obligations under the Privacy and Other Legislation Amendment Act 2024.

My name is [redacted]. I am a Responsible AI and Data Privacy governance professional holding the AIGP, CIPP/US, CIPP/E, CIPM, and CISM certifications, affiliated with Indiana Wesleyan University. I submitted the attached methodology — PAARA: Privacy-Aware AI Risk Architecture, Connector-DPIA Methodology v1.2 — to SSRN today (20 May 2026). The full paper is available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=6784078

The gap PAARA addresses:

The OAIC's October 2024 guidance on commercially available AI products recommends that deployers conduct a Privacy Impact Assessment before deployment and implement sensitivity-aware data handling. This is the right direction. However, the guidance — like equivalent guidance from every other authority surveyed — treats the AI product as the unit of analysis. It does not address the connector layer: the OAuth scopes, API integrations, and retrieval-augmented generation pipelines that link the AI product to the enterprise's internal data sources.

Most Australian enterprises deploying Microsoft 365 Copilot, Google Gemini for Workspace, or similar tools have not assessed the connector layer separately. Their PIA, if conducted at all, covers the vendor. It does not cover what the vendor's tool can reach through the connector, how retrieval boundaries are enforced, whether prompt injection via ingested enterprise content is possible, or how AI-mediated access amplifies insider risk.

PAARA provides a six-component practitioner methodology for this gap, including:

— A connector inventory and scope mapping template
— Application of PIA high-risk indicators at the connector layer
— An OAuth and API permission risk register
— A retrieval-boundary and prompt-injection threat model
— An insider-risk amplification assessment
— A cross-framework alignment table spanning Australian Privacy Principles, NIST AI 600-1, ISO/IEC 42005:2025, and EU AI Act Article 27

I would be grateful if OAIC would consider this methodology as practitioner input to the commercially available AI guidance review and the forthcoming ADM guidance. I am

happy to provide additional material or respond to questions.

Best regards,

[redacted]
AIGP | CIPP/US | CIPP/E | CIPM | CISM
Indiana Wesleyan University
SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=6784078